(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－355272

(43)公開日　平成11年(1999)12月24日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ	11/26	
12/56			11/20	１０２Ａ

審査請求　未請求　請求項の数14　ＯＬ　（全 19 頁）

(21)出願番号　特願平11－126563

(22)出願日　平成11年(1999)５月７日

(31)優先権主張番号　０９／０７４７４５

(32)優先日　1998年５月８日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600

(72)発明者　ムーイ　チョー　チュー
アメリカ合衆国　07724　ニュージャーシィ，イートンタウン，イートンクレスト　ドライヴ　148ビー

(74)代理人　弁理士　岡部　正夫　（外11名）

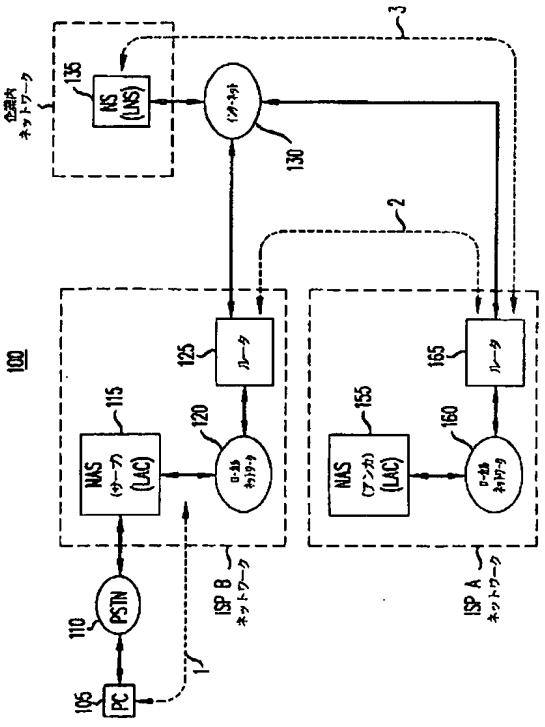
最終頁に続く

(54)【発明の名称】　多重ホップ・ポイント・ツー・ポイント・プロトコル

(57)【要約】

【課題】　本発明は、通信におけるパケット通信システムに関し、特に多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網（ＶＰＮ）サービスに関する技術を提供する。

【解決手段】　本発明は、パケット・サーバで使用される方法であって、他のパケット終端間に多重ホップ・パケット・トンネルを確立する段階と、該多重ホップ・パケット・トンネルを通じて該他のパケット終端間でメッセージを中継する段階とからなることを特徴とする。これにより、多数のインターネット・サービス・プロバイダ（ＩＳＰ）を通じて仮想ダイヤルアップ・サービスが提供され、特に、遠隔ユーザはサーブＩＳＰへの接続を確立することによって仮想ダイヤルアップ・サービスにアクセスする。サーブＩＳＰは、アンカＩＳＰへの第１トンネルを確立する。アンカＩＳＰは、例えば、私設イントラネットへのトンネルを確立する。その結果、多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網（ＶＰＮ）サービスが提供される。



【特許請求の範囲】

【請求項１】　パケット・サーバで使用される方法であって、該方法が、

他のパケット終端間に多重ホップ・パケット・トンネルを確立する段階と、

該多重ホップ・パケット・トンネルを通じて該他のパケット終端間でメッセージを中継する段階とからなることを特徴とする方法。

【請求項２】　請求項１に記載の方法において、該確立する段階が、

１つのパケット終端への第１のパケット・トンネルを確立する段階と、

別のパケット終端への第２のパケット・トンネルを確立する段階とからなることを特徴とする方法。

【請求項３】　請求項２に記載の方法において、該方法はさらに、接続情報を追跡する段階からなり、該接続情報は、該第１のパケット・トンネルに関するトンネル識別値と該第２のパケット・トンネルに関するトンネル識別値とを含む段階を含むことを特徴とする方法。

【請求項４】　請求項１に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に該メッセージの少なくとも一部を修正する段階を含むことを特徴とする方法。

【請求項５】　請求項１に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に該メッセージの少なくとも一部のトンネル識別情報を修正する段階を含むことを特徴とする方法。

【請求項６】　請求項１に記載の方法において、該中継段階は、該他のパケット終端間でメッセージを中継する前に、該パケット・サーバに関するパケット処理遅延を含む何れかのメッセージに含まれるパケット処理遅延情報を修正する段階を含むことを特徴とする方法。

【請求項７】　請求項１に記載の方法において、該パケット・サーバが多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする方法。

【請求項８】　請求項７に記載の方法において、該インターネット・プロトコルがレイヤ２トンネル・プロトコルの形態であることを特徴とする方法。

【請求項９】　パケット・ネットワークで使用される装置であって、該装置が、

ａ）仮想私設網サービスにアクセスするためにユーザとのポイント・ツー・ポイント・プロトコル接続を承認し、そしてｂ）ホップ間に配置されホップ間でメッセージを中継するように、他のパケット・サーバとの多重ホップ・トンネル接続を承認するパケット・サーバからなることを特徴とする装置。

【請求項１０】　請求項９に記載の装置において、該パケット・サーバは、該メッセージの少なくとも一部をホップ間で中継する前に修正することを特徴とする装置。

【請求項１１】　請求項９に記載の装置において、該パケット・サーバは、該メッセージの少なくとも一部のトンネル識別情報をホップ間で中継する前に修正することを特徴とする装置。

【請求項１２】　請求項９に記載の装置において、該パケット・サーバは、ホップ間でメッセージを中継する前に、該パケット・サーバに関するパケット処理遅延を含む何れかの該メッセージに含まれるパケット処理遅延情報を修正することを特徴とする装置。

【請求項１３】　請求項９に記載の装置において、該パケット・サーバは、多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする装置。

【請求項１４】　請求項１３に記載の装置において、該インターネット・プロトコルがレイヤ２トンネル・プロトコルの形態であることを特徴とする装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、概して、通信に関し、特にパケット通信システムに関する。尚、関連する主題が、本出願と同じ日付で出願された「移動ポイント・ツー・ポイント・プロトコル」という名称の特許出願で開示されている。

【０００２】通信手段としてのインターネットの用途の１つは、ワークグループを互いに結合していわゆる「仮想私設網」（Virtual Private Network：ＶＰＮ）を提供する高度データ・バックボーンとしての使用法である。ＶＰＮの応用例の１つは、従業員が、例えば、自宅でインターネットを通じて企業のデータ・ネットワークに遠隔アクセスできる企業環境におけるものである。ＶＰＮは、公衆設備を使用するにもかかわらず、閉じたユーザ・グループに参加する遠隔ユーザにセキュリティと認証を提供する。事実上、ＶＰＮを使用することによって、企業とその従業員にはＷＡＮと同様の手段が提供される（ユーザが直接企業のネットワークにダイヤルする等の方法で、企業のネットワークが直接遠隔アクセスを提供することもできるが、ＶＰＮを使用する方が経済的に有利である。）。

【０００３】ＶＰＮを提供するために、「ポイント・ツー・ポイント・トンネル・プロトコル」（Point-to-Poing Tunneling Protocol：ＰＰＴＰ）や「レイヤ２フォワーディング」（Layer 2 Forwarding）プロトコルといったトンネル・プロトコルが使用される。一般的に言って、トンネル・プロトコルは、１つのパケットを別のパケットの内部に配置することにより、公衆網を通じて専用データ・ストリームを作成することを可能にする。ＶＰＮの場合、ＩＰパケットが別のＩＰパケットの内部に配置される。業界標準の開発を目指して、インターネット・エンジニアリング・タスク・フォース（Internet Engineering Task Force：ＩＥＴＦ）は、「レイヤ２トンネル・プロトコル」（Layer 2 Tunneling

Protocol：Ｌ２ＴＰ）を開発しているが、これはＰＰＴＰとＬ２Ｆプロトコルの混成物である（例えば、K.Hamzeh、T.Kolar、M.Littlewood、G.Singh Pall、J.Taarud、A.J.Valencia及びW.Vertheinの「レイヤ２トンネルプロトコル" Ｌ２ＴＰ"（Layer Two Tunneling Protocol "L2TP"）」（Internet draft、1998年3月）を参照されたい。）。

【０００４】遠隔ユーザにとって、ＶＰＮにアクセスする通常の形態は、「在来型の電話サービス」（Plane-Old-Telephone Service:ＰＯＴＳ）接続により、ＶＰＮを提供する「インターネット・サービス・プロバイダ」（Ｉnternet Service Provider：ＩＳＰ）にアクセスすることである。例えば、ユーザは、アナログモデムをパーソナル・コンピュータまたはその相当品に組み込み、特定ＩＳＰ（ここでは「ホーム」ＩＳＰと呼ぶ）のカスタマ・アカウントを取得する（ユーザのパーソナル・コンピュータが上記のトンネル・プロトコルの１つをサポートするよう正しく設定されていることも前提となる）。ユーザは、「ホーム」ＩＳＰに関連する電話番号をダイヤルするなどして簡単にホームＩＳＰにデータ呼出を行った後ＶＰＮに「ログイン(logging in)」してＶＰＮにアクセスする。

【０００５】

【発明の概要】上記で説明したトンネル・プロトコルによっては、遠隔ユーザはＶＰＮにアクセスする際、ホームＩＳＰ以外のＩＳＰにはログインできないことが認識された。今日の移動通信の領域において、特にユーザが呼の継続中に物理的位置を変えるパーソナル・コミュニケーション・サービス（Personal Communication Service:ＰＣＳ）無線環境の場合、これは大きな制約である。言い換えれば、遠隔ユーザが位置を変える際、ホームＩＳＰは、少なくとも一時的にはユーザに利用できなくなり、ユーザのＶＰＮへのアクセスは阻止される。

【０００６】従って、本発明によれば、パケット・サーバは他のパケット終端間に多重ホップ・トンネルを確立し、多重ホップ・トンネルの部分間でメッセージを中継する。すなわち、遠隔ユーザは、ホームＩＳＰに加えて訪問中のＩＳＰによるＶＰＮへのアクセスが可能になる。

【０００７】本発明の実施例によれば、多数のインターネット・サービス・プロバイダ（ＩＳＰ）を通じて仮想ダイヤルアップ・サービスが提供される。特に、遠隔ユーザは、サーブＩＳＰ（serving ISP)への接続を確立することによって仮想ダイヤルアップ・サービスにアクセスする。サーブＩＳＰは、アンカＩＳＰへの第１トンネルを確立する。アンカＩＳＰは、例えば、私設イントラネットへのトンネルを確立する。その結果、多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網（Virtual Private Network：ＶＰＮ）サービスが提供される。

【０００８】

【発明の詳細な記述】すでに言及したように、本出願は、上記のＣｈｕａｈ他の特許出願に関連している。すなわち、詳細な説明は参照を容易にするため３つの節に分けられる。

【０００９】＜多重ホップ・ポイント・ツー・ポイント・プロトコル＞図１は、本発明の原理による例示としての通信システム１００を示す。本発明の概念以外、構成要素は周知であるので、詳細には説明しない。例えば、パーソナル・コンピュータ（Personal Computer:ＰＣ）１１０には、公衆電話網（Public-Switched-Telephone Network:ＰＳＴＮ）１１０を通じてＩＳＰ　Ｂにダイヤルアップ接続し、インターネット接続を確立するデータ通信機器（図示せず）が含まれる。同様に、通信システム１００の構成要素間の実線は対応する終端間の周知の通信機能を表している。例えば、ＰＣ１１０とＰＳＴＮ１１０間の接続は加入者回線接続を表し、ＩＳＰ　Ｂとインターネット１２０間の接続は同期光通信網（Synchronous Optical ＮＥTwork：ＳＯＮＥＴ）を通じて非同期転送モード（Asynchronous Transfer Mode:ＡＴＭ）によってサポートされる等である。さらに、読者は上記のＬ２ＴＰプロトコルに精通していることが前提になる。

【００１０】図１から見られるように、通信システム１００は、ＩＳＰ　Ａネットワークによって表されるＩＳＰ　Ａと、ＩＳＰ　Ｂネットワークによって表されるＩＳＰＢの２つのＩＳＰを備えている。ＩＳＰ　Ｂネットワークは、当業技術分野で周知の接続点（Point-Of-Presence：ＰＯＰ）ルータを含むネットワーク・アクセス・サーバ（Network Access Service:ＮＡＳ）１１５、ローカル・ネットワーク１２０およびルータ１２５を備えている。同様に、ＩＳＰ　Ａネットワークは、ＮＡＳ１５５、ローカル・ネットワーク１６０およびルータ１６５を備えている。ＩＳＰ　Ａが、例示としての企業のネットワークにネットワーク・サーバ（Network Server：ＮＳ）１３５を通じてアクセスする遠隔地に位置する従業員にＶＰＮサービスを提供することが想定されているが、このＮＳ１３５は多くの機能の中でも特に、ルーチングとファイアウォール機能を提供する（企業のネットワークは、例えば、ＮＳ１３５の背後で適切に保護されたローカルエリア・ネットワーク（図示せず）の集合であると想定される）。

【００１１】遠隔ユーザが、一時的にせよ、国内の、ＩＳＰ　ＡのサービスではなくｉｓｐＢのサービスの対象になる部分に位置することがあるのが観察された。さらに、ＩＳＰ　ＡがそのＶＰＮ対象範囲を他の範囲に拡大しようとすることがある。従って、本発明の原理によれば、遠隔ユーザは自分のホームまたはアンカＩＳＰに加えて訪問中またはサーブＩＳＰを通じてＶＰＮにアクセスすることができる（ＩＳＰ　ＡとＩＳＰ　Ｂが別のサ

ービス・プロバイダであることが想定されるが、これは必ずしも本発明の概念ではない。例えば、同じＩＳＰの中の別個のネットワークであってもよい）。すなわち、ＰＣ１０５に位置するユーザ（図示せず）は、国内を、例えば、移動しながら企業のネットワークにアクセスすることができる。

【００１２】この時点で、次の定義が前提となる。

ｍＬ２ＴＰ－ K.Hamzeh、T.Kolar、M.Littlewood、G.Singh Pall、J.Taarud、A.J.Valencia及びW.Vertheinの「レイヤ２トンネルプロトコル" L2TP" （LayerTwo Tunneling Protocol "L2TP"）」（Internet Draft、1998年3月）およびここで説明される修正によって定義されるＬ２ＴＰプロトコル。

ＬＡＣ－ｍＬ２ＴＰアクセス制御装置、すなわち、ｍＬ２ＴＰをサポートするＮＡＳ。

ＬＮＳ－ｍＬ２ＴＰをサポートするＮＳ。

アンカＬＡＣ－ＶＰＮサービスを提供するＬＮＳへのトンネルをサポートするＬＡＣ。

サーブＬＡＣ－アンカＬＡＣへのトンネルをサポートするＬＡＣ。

（これらの定義は本発明の概念の例示としての説明を単純化するために使用される。すなわち、当業者が認識するように、本発明の概念はこのように制限されるものではなく、あらゆるトンネル・プロトコルと関連処理機器に適用できる。）

【００１３】本発明の概念によれば、ＩＳＰ　Ａネットワークはアンカ１５５を示し、ＩＳＰ　Ｂネットワークはサーブ１１５を示す。以下さらに説明されるように、本発明の原理によれば、図１の通信システム１００は多重ホップ・トンネルを提供する。図１の例は、２つのホップ・トンネルを示す。１つのホップはＩＳＰ　Ｂネットワークから　Ａネットワークに至り、もう１つのホップはＩＳＰ　Ａネットワークから企業のネットワークに至っている。

【００１４】ここで図２を参照すると、本発明の原理による方法の高レベル流れ図が示される（サーブ１１５と他のそれぞれのサーバは、従来のプログラミング技術を使用して以下に説明する方法を実行するよう適切にプログラムされていると考えられるが、ここで使用されるプログラミング技術は周知のものなので説明しない）。ステップ２０５では、遠隔ユーザがＰＳＴＮ１１０を通じてＩＳＰ　ＢへのＰＰＰ（ポイント・ツー・ポイント・プロトコル）接続を開始する。ステップ２１０では、サーブ１１５が（例えば、所定の「ユーザ名」または「パスワード」を使用して）部分的にユーザを認証し、（図１の点線１で表される）接続を承認する（また、ＤＮＩＳ（Dialed Number Identification Service：ダイヤル番号識別サービス）、ＣＬＩＤ（Calling Line Identification：発呼回線識別）または他の同等の形態の識別法が使用されることもある）。明らかに、サーブ１１５がユーザを認証できない場合、接続は承認されない（このステップは図示されていない）。

【００１５】（背景として、また当業技術分野で周知のように、遠隔ユーザが新しいＰＰＰセッションの開始を希望する場合、ＰＣ１１０はサーブＬＡＣに対してＰＰＰＬＣＰ（Link Control Protocol：リンク制御プロトコル）構成要求(ConfigRequest)を開始する。本発明の概念によれば、サーブＬＡＣは、アンカＬＡＣとの通信を開始する前に、ユーザの機器と、当業技術分野で周知のように、ＰＰＰＬＣＰとＰＰＰ　ＰＡＰ／ＣＨＡＰ両方の段階を完了する。（安全なコンジットのために、ＩＥＴＦは、パスワード認証プロトコル（Password Authentication Protocol：ＰＡＰ）とチャレンジーハンドシェーク認証プロトコル（Challenge-Handshake Authentication Protocol：ＣＨＡＰ）という、ＰＰＰ接続のセキュリティのための２つのプロトコルを定義した（例えば、IETF Request forComment（ＲＦＣ）１３３４、「ＰＰＰ認証プロトコル」を参照されたい。））

【００１６】ステップ２１５では、サーブＬＡＣ１１５が、遠隔ユーザがＶＰＮサービスの使用を希望していると判断する（この選択は、特定の「ユーザ名」に直接関連し、および／または、例えば、サービスＬＡＣ１１５が提供するポップアップ「ハイパーテキスト・トランスポート・プロトコル（Hyper Text Transfer Protocol：ＨＴＴＰ）フォームによるなどの、ユーザからの個別の要求に関連する」。遠隔ユーザが仮想ダイヤルアップ・サービスを要求しない場合、サーブＬＡＣ１１５はステップ２２０で標準インターネット・アクセスを提供する。しかし、遠隔ユーザがＶＰＮの使用を希望する場合、サーブＬＡＣ１１５はステップ２２５で関連するアンカＬＡＣを特定する（以下説明する）。

【００１７】サーブＬＡＣ１１５は、例えば、ユーザのＩＤを特定のアンカＬＡＣにアプリオリに関連づけるＶＰＮテーブルを保存している。こうしたテーブルの一部を以下表１に示す。この例では、ＰＣ１１０に関連する遠隔ユーザが、アンカＬＡＣであるＩＳＰＡ．ｃｏｍ、すなわちアンカＬＡＣ１５５に関連している。

【表１】

ユーザＩＤ	アンカーＬＡＣ
ユーザ名	ＩＳＰＡ．ｃｏｍ

表１

【００１８】（単に“ユーザ名@ＩＳＰＡ．ｃｏｍ”といった形で構成されたフィールドのリストを維持するといった同等の構造または操作が使用されることもあることに留意されたい。なお、ここでは@記号の後の部分はアンカＬＡＣを示す。また、ＩＳＰ　Ｂがユーザをサービスにマップするデータベースを維持することもある。仮想ダイヤルアップ、すなわち、遠隔ユーザをＶＰＮサ

ービスに関連するものとして特定する場合、このマッピングはさらにアンカＬＡＣを特定する。また、当業技術分野で周知のように、サーブＬＡＣはこのタスクのためにローカルラディアスサーバ(local radius server)とのラディアスアクセス要求／応答トランザクションを使用することもある）

【００１９】ステップ２３０では、サーブＬＡＣ１１５が、サーブＬＡＣ１１５自体とアンカＬＡＣ１５５の間にトンネルがあるかを確認する。すなわち、サーブＬＡＣ１１５は、トンネル識別（Tunnel identification：Ｔｉｄ）値、現在そのトンネルを使用する呼の関連呼識別子（Call identifiers:Ｃｉｄ）および関連するアンカＬＡＣのＩＰアドレスによって表される現行トンネルの、以下表２で示されるようなテーブルを保守する。

【表２】

Ｔｉｄ	Ｃｉｄ	アンカーＬＡＣ　ＩＰアドレス
2	5	h．j．k．l

表２

【００２０】サーブＬＡＣとアンカＬＡＣの間にトンネル接続が現在存在しない場合、ステップ２３５で、サーブＬＡＣ１１５によってアンカＬＡＣへのトンネルが確立される（以下説明する）。サーブＬＡＣとアンカＬＡＣの間にトンネルが存在する場合、サーブＬＡＣ１１５は、ステップ２４０で、新しいＣｉｄを割り当て、表２を更新し、（以下さらに説明するように）ローカル・ネットワーク１２０、ルータ１２５、インターネット１３０、ルータ１６５およびローカル・ネットワーク１６０を通じてＶＰＮ要求をアンカＬＡＣ１５５に転送する。この要求の中で、サーブＬＡＣ１１５はユーザ識別情報をアンカＬＡＣ１５５に伝える。

【００２１】ここで図３を参照すると、アンカＬＡＣ１５５はステップ３０５で要求を受信する。ステップ３１０では、アンカＬＡＣ１５５はさらに（例えば、上記で言及した所定の「ユーザ名」と「パスワード」を使用して）遠隔ユーザの認証を行い、（図１の点線２で表される）接続を承認する（また、サーブＬＡＣと同様、ＤＮＩＳ、ＣＬＩＤまたは他の同等の形態の識別が使用されることもある）。アンカＬＡＣ１５５がユーザを認証できない場合、接続は承認されない（このステップは図示されていない。この場合、サーブＬＡＣ１１５は同様にエラーメッセージを遠隔ユーザ（図示せず）に返送しなければならない。）。

【００２２】アンカＬＡＣ１５５は、例えば、ユーザのＩＤを特定のＬＮＳにアプリオリに関連づけるＶＰＮテーブルを保存している。こうしたテーブルの一部を以下表３に示す。この例では、ＰＣ１１０に関連する遠隔ユーザが、ＩＰアドレスg．h．i．jによって表されるＬＮＳ１３５に関連している。

【表３】

ユーザＩＤ	ＬＮＳ
ユーザ名	g．h．i．j

表３

【００２３】（サーブＬＡＣ１１５と同様に、同等の構成または動作が使用できることに留意されたい。例えば、アンカＬＡＣは、ホームラディアスサーバ(Home Radius Server)により、ラディアスアクセス要求／応答メッセージを通じてこの機能を行うことがある。）ステップ３１５では、アンカＬＡＣ１５５は、表３を使用してこれが有効な要求かを確認する。これが有効な要求でない場合、アンカＬＡＣ１５５はステップ３２０で要求を拒否する。これが有効な要求である場合、アンカＬＡＣはステップ３２５で表３から関連ＬＮＳを識別する。

【００２４】アンカＬＡＣは、遠隔ユーザとの間に確立された各ＶＰＮセッションについて、各通信方向に関する次の接続テーブルを保守していると想定される。

【表４】

	サーブLAC		サーブLAC	LNS		LNS	ユーザに割り当てられたIPアドレス
接続番号	Tid	Cid	IPアドレス	Tid	Cid	IPアドレス	
5	2	5	d.e.f.g	1	3	g.h.i.j	a.b.c.d

表４

【００２５】アンカＬＡＣは、接続番号を各ＶＰＮセッションに関連づける。さらに、この接続番号は対応するユーザにマップ(map)される。この表は、接続番号によって、（そのホップの関連トンネルＩＤと呼ＩＤ値を伴う）サーブＬＡＣのＩＰアドレスと、（その関連するホップの関連トンネルＩＤと呼ＩＤ値を伴う）関連ＬＮＳのＩＰアドレスを列挙する。ステップ３３０では、アンカＬＡＣ１５５がＶＰＮセッションを確立する（認証の確認等を行う）。（ここでも、ＬＮＳ１３５が（例えば、遠隔ユーザの認証ができない場合や遠隔ユーザを受け入れる余地がないために）ＶＰＮ要求を拒否した場合、アンカＬＡＣとサーブＬＡＣによって適当なエラーメッセージが生成される）。本発明の概念以外に、ＬＮＳ１３５とのＶＰＮセッションが当業技術分野で周知の

ように確立される。例えば、本発明の原理によれば、新しいＶＰＮセッションを確立する際に、アンカＬＡＣ１５５は新しいＣｉｄを割り当て、表４を更新する（例えば、新しい接続を割り当てる）。この最後の接続は、図１の点線３によって表される。

【００２６】この時点で、連結性はポイント・ツー・ポイントＰＰＰセッションであり、その終端は、一方では（ＰＣ１１０によって表される）遠隔ユーザのネットワーク・アプリケーションであり、もう一方ではこの連結性のＬＮＳ１３５ＰＰＰサポートへの終端である（必要な場合、ＬＮＳと共にサーブＬＡＣ、アンカＬＡＣで課金処理を行えることに留意されたい。すなわち、各構成要素はパケット、オクテット、接続の開始・終了時間をカウントすることができる）。

【００２７】上記の多重ホップ仮想ダイヤルアップ・サービスをサポートする目的で、ある形式のＬ２ＴＰ（ｍＬ２ＴＰ）プロトコルが使用されるが、これについて以下説明する。Ｌ２ＴＰでは、各ＬＡＣ－ＬＮＳペア間の制御メッセージと、同じＬＡＣ－ＬＮＳペア間のペイロード・パケットという所定のトンネルで動作するｍＬ２ＴＰの２つの並列コンポーネントが存在する。後者は、ＬＡＣ－ＬＮＳペア間のユーザ・セッションに関するｍＬ２ＴＰカプセル化ＰＰＰパケットを転送する。Ｌ２ＴＰでは、Ｎｒ（次の受信）およびＮｓ（次の送信）フィールドが常に制御メッセージに表示され、必要に応じてペイロード・パケットに存在する。制御メッセージとペイロード・メッセージは別のシーケンス番号状態を使用する。上記のＬＡＣ／ＬＮＳペアのシナリオでは、（Ｎｒ、Ｎｓ）の保守と使用に関する限りＬ２ＴＰドラフト・プロトコル定義の変更はない。

【００２８】しかし、サーブＬＡＣとアンカＬＡＣの間の接続では、アンカＬＡＣはサーブＬＡＣが送信する（Ｎｒ、Ｎｓ）値を監視するだけである。すなわち、本発明の概念によれば、アンカＬＡＣは単純にサーブＬＡＣから受信した値をＬＮＳに再送信する。さらに、アンカＬＡＣはここで、サーブＬＡＣが送信したパケットから観察された対応する（Ｎｒ、Ｎｓ）値によって（受信状態、送信状態）値（Ｓｒ、Ｓｓ）を更新する。サーブＬＡＣとアンカＬＡＣの間には疑いなくパケット損失が存在するので、アンカＬＡＣのＳｓ（Ｓｒ）値はサーブＬＡＣのＳｓ（Ｓｒ）値より小さい（小さい）。さらに、アンカＬＡＣは、サーブＬＡＣ／アンカＬＡＣ制御接続に関するものと、アンカＬＡＣ／ＬＮＳ制御接続に関するものとの２組の（Ｓｒ、Ｓｓ）変数を保守する。

【００２９】ＰＰＰトンネルが形成される前に、本発明の概念によれば、サーブＬＡＣ、アンカＬＡＣおよびＬＮＳの間で制御メッセージを交換しなければならない。制御メッセージは、後にｍＬ２ＴＰ呼制御管理情報が伝えられた場合ペイロード・データの転送に使用されるのと同じトンネルを通じて交換される（後で説明する）。

【００３０】本発明の概念によれば、追加属性値ペア（addtional Attribute Value Pairs:additional ＡＶＰ）（後で説明する）が定義され、Ｌ２ＴＰ制御メッセージ（ひいてはｍＬ２ＴＰ制御メッセージとなる）で使用される。この追加ＡＶＰは上記で説明した多重ホップ機能と呼転送機能をサポートするためのものである。Ｌ２ＴＰの定義では、ＡＶＰはさらに制御信号を指定するためにも使用される。

【００３１】上記で言及したように、上記で説明したＬＡＣ／ＬＮＳペアの場合、上記で言及したＬ２ＴＰドラフトで説明した手順に変更はない。すなわち、以下説明する追加手順が必要になるのは、多重ホップの場合だけである。

【００３２】多重ホップ・メッセージの流れの例を図４に示す。図４から観察されるように、サーブＬＡＣとアンカＬＡＣの間にトンネル（Ｔｉｄ値で示される）と呼（Ｃｉｄ値で示される）が確立される。同様に、アンカＬＡＣとＬＮＳの間にトンネルと呼が確立される。図４に示すように、本発明の概念はサーブＬＡＣがアンカＬＡＣへのトンネルを確立することを要求する。本発明では、サーブＬＡＣはアンカＬＡＣをＬＮＳとして扱い、Ｌ２ＴＰ手順が使用されてトンネルを初期設定する。

【００３３】トンネルが確立されると、多数の制御メッセージ・トランザクションが発生し、本発明の原理によってＰＰＰセッションを設定する。それらは図５－図７に示される。これらの図では、様々な制御メッセージの関連フィールドだけが図示される（サーブＬＡＣとアンカＬＡＣ間のトンネルのトンネルｉｄおよび呼ｉｄが、アンカＬＡＣとＬＮＳ間のそれらの数値と異なっている場合、アンカＬＡＣはそれらを何れかの方向に中継する前にパケット・ヘッダの関連フィールドを修正する）。

【００３４】図５に示すように、サーブＬＡＣはまず開始制御接続一要求(Start-Control-Connect-Request Message(SCCRQ))メッセージ（Ｌ２ＴＰの定義による）をアンカＬＡＣに送信し、両者間にトンネルを設定する。このメッセージを受信すると、アンカＬＡＣは開始制御接続一応答(Start-control-Connect-Reply Message(SCCRP))によって応答する（これは上記で説明した何らかの認証に続いて行われる）。サーブＬＡＣは開始制御接続一接続(Start-Control-Connection-Connect(SCCCN))メッセージによってアンカＬＡＣに対する確認を行う。

【００３５】図５に示す開始制御接続(Start-Control-Connection)メッセージの交換に続いて、サーブＬＡＣは、図６に示すように、着信呼要求(Incoming-Call-Request(ICRQ))メッセージをアンカＬＡＣに送信する。着信呼要求(Incoming-Call-Request)メッセージにはアンカＬＡＣがＬＮＳを識別するのに十分なユーザ・データと信用証明が含まれている。

【００３６】前に述べたように、アンカＬＡＣとＬＮＳの間にトンネルが存在しない場合、アンカＬＡＣは、Ｌ

２ＴＰの定義により、ＬＮＳとのＳＣＣＲ、ＳＣＣＲＰ、ＳＣＣＣＮメッセージ交換を開始する。トンネルが存在する場合、トンネル内の未使用スロットであるＣｉｄがアンカＬＡＣによって割り当てられる。この時点で、本発明の原理によれば、アンカＬＡＣはＩＣＲＱメッセージを（サーブＬＡＣから）中継し、ＬＮＳにこの新しいダイヤルアップ・セッションについて通知する。図６に示すように、アンカＬＡＣはＩＣＲＱメッセージをＬＮＳに中継する前にしかるべく修正する。修正されたフィールド、例えば、割当て呼ＩＤは、“*”によって示される。アンカＬＡＣはまた隠しＡＶＰを追加し、ＬＮＳにサポート可能な受信ウィンドウ・サイズを知らせる（追加ホップの場合、アンカＬＡＣは制御／ペイロード両方の接続について取り決められた最大ウィンドウ・サイズを記録することに留意されたい。また、サーブＬＡＣとアンカＬＡＣ間の制御接続のウィンドウ・サイズがアンカＬＡＣとＬＮＳ間の制御接続のものと異なっており、バッファリングが必要なことがある。バッファリングとシーケンス番号監視の追加を避けるために、アンカＬＡＣは必要に応じて、アンカＬＡＣがアンカＬＡＣからサーブＬＡＣの方向でサポートできるペイロード・セッション用の受信ウィンドウ・サイズをＬＮＳに知らせるＡＶＰを追加する。その結果、ＬＮＳは、ＩＣＲＰ応答の適当な受信ウィンドウ・サイズ値だけを含み、ひいてはＬＮＳ－アンカＬＡＣ－サーブＬＡＣ方向のペイロード・セッションのための１つのウィンドウ・サイズだけを含むことになる。）。

【００３７】前に述べたように、ＬＮＳは接続を承認または拒否する。拒否は結果状態を含まなければならず、エラー表示を含むことがある。どちらの場合でも、ＬＮＳは、図６に示すように、着信呼応答(Incoming-Call-Reply(ICRP))メッセージをアンカＬＡＣに送信する。本発明によれば、次にアンカＬＡＣはＩＣＲＰメッセージを適当に修正し、サーブＬＡＣに中継する（やはり、修正されたフィールドは図６では“*”で示される）。ＬＮＳから受信されたパケット処理遅延（ＰＰＤ）フィールドにはＬＮＳの処理遅延だけが含まれるので、アンカＬＡＣはこの値にそれ自体のノードの処理遅延を追加する。次に、ＩＣＲＱメッセージがサーブＬＡＣに中継される。

【００３８】それに応答して、サーブＬＡＣは、図７に示すように、着信呼接続(Incoming-Call-Connected(ICCN))メッセージをアンカＬＡＣに送信する。このメッセージの中で、サーブＬＡＣはすべてのＬＣＰ構成要求(Config Request)情報をプロキシ認証情報(Proxy Authentification Information)と共に伝える。すなわち、サーブＬＡＣはユーザの機器で行われたＬＣＰ構成要求／応答(Config Request/Ack)、ＰＰＰ　ＰＡＰ／ＣＨＡＰの結果を転送する。アンカＬＡＣは、受信ＩＣＣＮメッセージのＰＰＤフィールドをＬＮＳに中継する前に修正する（現在、送信接続速度と受信接続速度は使用されない）。図示されていないが、本発明によれば、アンカＬＡＣはＬ２ＴＰで定義されたすべてのSet-Link-Info、HelloおよびWan-Error-Notifyメッセージをも中継する（上記の説明は多重ホップ・パケット・トンネルの概念を示すものであることが観察されるだろう。例えば、図１は２ホップ・パケット・トンネルを表している）。

【００３９】上記で説明した多重ホップｍＬ２ＴＰトンネルはもっぱらフレーム層で発生することが観察されるだろう。すなわち、どんな目的のＰＰＰプロトコル処理でも、遠隔ユーザはＬＮＳと接続するように見えるので、ＬＮＳによるアドレス管理の実際の方法は上記で説明した仮想(Virtual)ダイヤルアップ・サービスとは無関係である。

【００４０】＜移動ポイント・ツー・ポイント・プロトコル＞ここで図８を参照すると、本発明の概念の他の実施例が示される。図８は図１と同様である。本発明の概念以外、構成要素は周知であるので、詳細には説明しない。同じ数字は同じ機能を示し、必要な場合以外それ以上説明しない。

【００４１】図８では、ＰＣ８０５には、パーソナル・コミュニケーション・サービス（ＰＣＳ）無線ネットワーク８１０を通じてインターネットへの無線アクセスを確立するデータ通信機器（図示せず）が含まれる。ＰＣＳ無線ネットワークは当業技術分野で周知であるので詳細には説明しない。ＰＣＳ無線ネットワーク８１０は、要素８１５および８２０で表されるような複数の移動交換センタを備えている。各交換センタはある地理的範囲（図示せず）にサービスを提供する。要素８１５と８２０にはＮＡＳが含まれることが想定され、例えば、サーブＬＡＣは図１のサーブＬＡＣ１１５と同様である。まず、遠隔ユーザが上記で説明した多重ホップ技術を使用して企業のネットワークへのＶＰＮセッションを確立することが想定される。すなわち、遠隔ユーザは、この初期接続が要素８１５を通じて接続８１４と８１６により転送されるような地理的範囲にある。無線ＰＣＳ用の場合、初期ＰＰＰ接続は要素８１５とＰＣ８０５の間で行われる（簡単にするために交換要素の一部として示されているが、ＮＡＳ機能は機器の独立した部分でも行われる。同様に、ローカル・ネットワークやルータといった他の要素も簡単にするために図示しない。）。

【００４２】無線環境では、Ｌ２ＴＰのようなトンネル・プロトコルによっては遠隔ユーザが既存のＰＰＰ接続を１つの交換要素から他の交換要素に変更できないということが認識された。例えば、図８が本発明の概念を実施しないことを想定すると、遠隔ユーザが要素８２０（ひいては異なったＮＡＳ）のサービスの対象となる地理的範囲に移動する場合、ユーザの通信セッションは、当業技術分野で周知のように要素８２０に受け渡される。しかし、すでに述べたように、既存のＰＰＰ接続を

１つのＮＡＳから別のＮＡＳに転送することはできないため、既存のＰＰＰ接続（ひいてはＶＰＮセッション）は中断し、復旧しなければならなくなる。この場合、図８の通信システムはこの問題を克服する。

【００４３】従って、本発明によれば、ＮＡＳまたはＬＡＣは、既存のＮＡＳが既存のＰＰＰ接続を別のＮＡＳにハンドオフできるようにする「ハンドオフ」機能を組み込んでいる。この機能によれば、(ｉ)継続呼要求(Continued Call Request)、(ii)継続呼応答(Continued Call Reply)および(iii)継続呼接続(Continued Call Connect）という３つの新しい制御メッセージが定義される。上記の結果、ユーザは現行のＰＰＰ接続を終了してから新しいＰＰＰ接続を復旧する必要はない。この３つの制御メッセージは、Ｌ２ＴＰ制御メッセージ・ヘッダ、メッセージ識別子（例えば、継続呼要求等）および多数のフィールド（後で説明する）を含んでいる。

【００４４】本発明の概念による、ハンドオフ・メッセージの流れの例を図９に示す。図９から観察されるように、トンネル（Ｔｉｄ値で示される）と呼（Ｃｉｄ値で示される）がまず要素８１５（ここにはサーブＬＡＣが含まれる）とアンカＬＡＣの間に確立される。同様に、アンカＬＡＣとＬＮＳの間にトンネルと呼が確立される（この初期ＶＰＮセッションを確立する方法は上記で説明済みである）。図９に示すように、本発明の概念によれば、既存のサーブＬＡＣは既存のＰＰＰ接続を、要素８２０によって表されるような新しいサーブＬＡＣに転送することができる。

【００４５】ここで、「ハンドオフ機能」を提供する際使用される方法の流れ図の例である図１０を参照されたい。すでに述べたように、ＰＣ８０５と企業のネットワークの間に要素８１５を通じたＶＰＮセッションが存在し、そこにサーブＬＡＣとアンカＬＡＣ１５５が含まれることが想定される。本発明の概念によれば、ＰＣＳ無線ネットワーク８１０は既存の呼状態変数に、各無線呼に関するＰＰＰ接続の存在（または存在しないこと）を示す追加変数を追加し、ＰＰＰ接続が存在する場合、例えば、アンカＬＡＣのＩＰアドレスであるアンカＬＡＣのＩＤを含むＰＰＰ接続情報を追加する。

【００４６】図１０のステップ４０５では、ＰＣＳ無線ネットワーク８１０は、ＰＣ８０５が要素８１５のサービスの対象になる地理的範囲から別の地理的範囲、例えば、要素８２０のサービスの対象になり、別のサービスＬＡＣが含まれる範囲に移動したためハンドオフが必要になったことを検出する。ステップ４１０では、ＰＣＳ無線システムは要素８２０にハンドオフが迫っていることを通知する（ハンドオフを検出し遂行するために無線システムが使用する方法は当業技術分野で周知であり、本発明の概念には関連しない。従って、それらはここでは説明されず、図８の信号経路８１１で表される）。ここで、呼状態情報にはＰＰＰセッション識別子とＰＰＰ呼情報が含まれているので、（要素８２０の）新しいサーブＬＡＣはステップ４１５でアンカＬＡＣを識別する。ステップ４２０で、（要素８２０の）新しいサーブＬＡＣはそれ自体と識別されたアンカＬＡＣ（ここではアンカＬＡＣ１５５）の間にすでにトンネルがあるかを確認する。

【００４７】トンネルがない場合、新しいサーブＬＡＣはまずステップ４２５で（前に説明されたように）トンネルを確立する。次に、本発明の概念によれば、新しいサーブＬＡＣはステップ４３０で継続呼要求(Continued-Call-Request(CCRQ))メッセージをアンカＬＡＣに送信する。このＣＣＲＱメッセージには、既存のＰＰＰ接続に関連するユーザ名、移転先の（新しい）ＰＰＰセッションで使用されるＴｉｄとＣｉｄの値が含まれる。

【００４８】ステップ４３５では、アンカＬＡＣは受信したＣＣＲＱメッセージからユーザ名を回復し、この情報を使用して古いサーブＬＡＣのＬＮＳとＩＰアドレスを、例えば、上記の表４で表される接続テーブルから判定する（この回復された情報には対応するユーザ・データグラム・プロトコル（User Datagram Protocol：ＵＤＰ）ポート番号が含まれることもある）。このステップでは、アンカＬＡＣは呼切断通知(Call-Disconnect-Notify)メッセージ（例えば、Ｌ２ＴＰ参照）を古いサーブＬＡＣに送信し、かつ、例えば、上記の表４で、古いトンネルｉｄや古い呼ｉｄといった遠隔ユーザへのこのＰＰＰ接続に関連する既存の呼変数を識別する（他方、アンカＬＡＣが継続呼要求(Continued-Call-Request)を拒否した場合、サーブＬＡＣは、既存のＰＰＰセッションが切断され、新しいＰＰＰセッションが開始されるか、または単にＰＰＰセッションが中止されるように信号を返送する（このステップは図示しない））。

【００４９】ステップ４４０では、アンカＬＡＣが適当な受信ウィンドウ・サイズで継続呼応答(Continued-Call-Reply：CCRP)メッセージによって応答する。ＣＣＲＰメッセージには現行のＮｒとＮｓの値に関する情報が含まれる。ステップ４４５では、（ステップ４３５で識別された）Ｔｉｄ、ＣｉｄおよびサーブＬＡＣのＩＰアドレス・フィールドのエントリを既存のＰＰＰ接続の新しい呼情報に置換することにより、接続テーブル（例えば、上記の表４）を更新する。ステップ４５０では、新しいサーブＬＡＣはＮｒ、ＮｓをＳｒ、Ｓｓ値に保存し、かつ必要な場合受信したＣＣＲＰメッセージから受信ウィンドウ・サイズを保存し、継続呼接続（Continued-Call-Connect：CCCN)メッセージをアンカＬＡＣに送信し、これをもってハンドオフを完了する。

【００５０】ＰＰＰプロトコルの上記で説明したハンドオフ機能を裏付けるものとして、図１１は本発明の原理による上記で言及した新しい制御メッセージ・トランザクションの例を示す。図１１に示すように、ＣＣＲＱメッセージが識別されたアンカＬＡＣに送信される。

【００５１】ＣＣＲＱメッセージは次のフィールドを含む。
－割当てＣｉｄ
－呼シリアルナンバー
－ベアラ(bearer)の種類
－物理チャネルＩＤ
－ダイヤルされた番号
－ダイヤルする番号
－副アドレス
－アンカＬＡＣ
－チャレンジ
－ユーザＡＶＰ
－ユーザ名
－ユーザのＭＩＮ／電話番号
【００５２】アンカＬＡＣのフィールドは、この情報がハンドオフの際に利用可能であることを想定している（また、ハンドオフ処理がアンカＬＡＣに関する情報を新しいサーブＬＡＣに提供しない場合、ハンドオフ処理は、当業技術分野で周知のように新しいサーブＬＡＣが外部ラディアスサーバの助けによってアンカＬＡＣ情報を検索する十分なユーザ情報を新しいサーブＬＡＣに提供しなければならない。すなわち、新しいサーブＬＡＣはラディアスアクセス／応答メッセージにより、ホームラディアスサーバからアンカＬＡＣについて照会する）。
【００５３】ユーザＡＶＰ情報には（ユーザ名のような）ユーザ情報と、例えば、多重ホップ仮想ダイヤルアップ・サービス、ユーザのＩＤ（ＭＩＮ）、サービス・プロバイダの電話番号等といった他のユーザの信用証明が含まれる。
【００５４】ＣＣＲＱメッセージに続いて、アンカＬＡＣは呼切断通知(Call-Disconnect-Notify)メッセージを古いサーブＬＡＣに送信する。次に、アンカＬＡＣは、保守の対象となる現行Ｓｒ、Ｓｓを含む継続呼応答(Continued-Call-Reply：CCRP)メッセージによって応答する。
【００５５】ＣＣＲＰメッセージは次のフィールドを含む。
－割当てＣｉｄ
－結果コード
－受信ウィンドウ・サイズ
－ＰＰＤ
－Ｎｒ
－Ｎｓ
－チャレンジ
－チャレンジ応答
【００５６】最後に、新しいサーブＬＡＣが継続呼接続(Continued-Call Connect：CCCN)によって応答する。ＣＣＣＮメッセージは次のフィールドを含む。
－接続速度
－フレーム種類
－受信ウィンドウ・サイズ
－ＰＰＤ
－チャレンジ応答
【００５７】ここで図１２を参照すると、既存のＰＰＰ接続を１つのＮＡＳから別のＮＡＳに移転し、その際古いＮＡＳがＬＮＳに接続している場合、本発明の概念の他の実施例が示される（この例では、サーブＬＡＣは本質的に存在せず、例えば、もっと簡単に、アンカＬＡＣが既存のＰＰＰ接続を直接サポートする）。図１２は図８と同様である。本発明の概念以外、構成要素は周知であるので、詳細には説明しない。同じ数字は同じ機能を示し、必要な場合以外それ以上説明しない。
【００５８】図１２では、ＰＣ８０５には、パーソナル・コミュニケーション・サービス（Personal Communication Service:ＰＣＳ）無線ネットワーク９１０を通じてインターネットへの無線アクセスを確立するデータ通信機器（図示せず）が含まれる。ＰＣＳ無線サービスは当業技術分野で周知であるので詳細には説明しない。ＰＣＳ無線ネットワーク９１０は要素８７５および８８０で表されるような複数の移動交換センタを含む。各交換センタはある地理的範囲（図示せず）にサービスを提供する。要素８７５と８８０には、例えば、図１のアンカＬＡＣ１１５と同様のＬＡＣであるＮＡＳが含まれる。まず、遠隔ユーザが、例えば、Ｌ２ＴＰの該当部分を使用して、当業技術分野で周知のように企業のネットワークへのＶＰＮセッションを確立することが想定される。すなわち、遠隔ユーザはこの最初の接続が要素８７５を通じて接続８７４と８７６によりＬＮＳ９３５に転送されるような地理的範囲にある。無線ＰＣＳ適用業務の場合、初期ＰＰＰ接続は要素８７５とＰＣ８０５の間で行われる（簡単にするために交換要素の一部として示されているが、ＮＡＳ機能は機器の独立した部分でも行われる。同様に、ローカル・ネットワークやルータといった他の要素も簡単にするために図示しない）。
【００５９】この実施例では、上記で説明したＣＣＲＱ、ＣＣＲＰ、ＣＣＣＮメッセージが新しいＬＡＣとＬＮＳの間で交換される点以外は、同じハンドオフ手順がＬＡＣ／ＬＮＳペアについて実行される。本発明の概念による、ハンドオフ・メッセージの流れの例を図１３に示す。図１３から観察されるように、トンネル（Ｔｉｄ値で示される）と呼（Ｃｉｄ値で示される）がまず要素８７５（ここにはＬＡＣが含まれる）とＬＮＳ９３５の間に確立される。図１３に示すように、本発明の概念は、既存のＬＡＣが既存のＰＰＰ接続を、要素８８０で表される新しいＬＡＣに移転することを可能にする。
【００６０】ここで、「ハンドオフ機能」を提供する再使用される方法の流れ図の例である図１４を参照されたい。すでに述べたように、ＰＣ８０５と企業のネットワークの間に、ＬＡＣを含む要素８７５を通じてＶＰＮセ

ッションが存在していることが想定される。本発明の概念によれば、ＰＣＳ無線ネットワーク９１０は既存の呼状態変数に、各無線呼に関するＰＰＰ接続の存在（または存在しないこと）を示す状態変数を追加し、ＰＰＰ接続が存在する場合、例えば、ＬＮＳのＩＰアドレスであるＬＮＳのＩＤを含むＰＰＰ接続情報を追加する。

【００６１】図１４のステップ５０５では、ＰＣＳ無線ネットワーク９１０は、ＰＣ８０５が要素８７５のサービスの対象になる地理的範囲から別の地理的範囲、例えば、要素８８０のサービスの対象になり、別のサービスＬＡＣが含まれる範囲に移動したためハンドオフが必要になったことを検出する。ステップ５１０では、ＰＣＳ無線システムは要素８８０にハンドオフが迫っていることを通知する（ハンドオフを検出し遂行するために無線システムが使用する方法は当業技術分野で周知であり、本発明の概念には関連しない。従って、それらはここでは説明されず、図１２の信号経路９１１で表される）。ここで、呼状態情報にはＰＰＰセッション識別子とＰＰＰ呼情報が含まれているので、（要素８８０の）新しいＬＡＣはステップ５１５でアンカＬＡＣを識別する。ステップ５２０で、（要素８８０の）新しいＬＡＣはそれ自体と識別されたＬＮＳ（ここではＬＮＳ９３５）の間にすでにトンネルがあるかを確認する。

【００６２】トンネルがない場合、新しいＬＡＣはまずステップ５２５で（前に説明されたように）トンネルを確立する。次に、本発明の概念によれば、新しいＬＡＣはステップ５３０で継続呼要求(Continued-Call-Request：CCRQ)メッセージをＬＮＳに送信する。このＣＣＲＱメッセージには、既存のＰＰＰ接続に関連するユーザ名、移動先の（新しい）ＰＰＰセッションで使用されるＴｉｄとＣｉｄの値が含まれる。

【００６３】ステップ５３５では、ＬＮＳは受信したＣＣＲＱメッセージからユーザ名を回復し、この情報を使用して古いＬＡＣのＩＰアドレスを判定する（この回復された情報には対応するユーザ・データグラム・プロトコル（ＵＤＰ）ポート番号が含まれることもある）。このステップでは、アンカＬＡＣは呼切断通知(Call-Disconnect-Notify)メッセージ（例えば、Ｌ２ＴＰ参照）を古いＬＡＣに送信し、かつ、例えば、上記の表４で示されるものと同様だが、サーブＬＡＣ情報等は除く接続テーブルで、古いトンネルｉｄや古い呼ｉｄといった遠隔ユーザへのこのＰＰＰ接続に関連する既存の呼変数を識別する（他方、ＬＮＳが継続呼要求(Continued-Call-Request)を拒否した場合、新しいＬＡＣは、既存のＰＰＰセッションが切断され、新しいＰＰＰセッションが開始されるか、または単に古いＰＰＰセッションが中止されるように信号を返送する（このステップは図示しない））。

【００６４】ステップ５４０では、ＬＮＳが適当な受信ウィンドウ・サイズで継続呼応答(Continued-Call-Reply：CCRP)メッセージによって応答する。ＣＣＲＰメッセージには現行のＮｒとＮｓの値に関する情報が含まれる。ステップ５４５では、ＬＮＳは、（ステップ５３５で識別された）Ｔｉｄ、ＣｉｄおよびＬＡＣのＩＰアドレス・フィールドのエントリを既存のＰＰＰ接続の新しい呼情報に置換することにより、接続テーブルを更新する。ステップ５５０では、新しいＬＡＣはＮｒ、Ｎｓを更新し、必要な場合受信したＣＣＲＰメッセージからＮｒ、Ｎｓと受信ウィンドウ・サイズを更新し、継続呼接続(Continued-Call-Connect：CCCN)メッセージをＬＮＳに送信し、これをもってハンドオフを完了する。

【００６５】ＰＰＰプロトコルの上記で説明したハンドオフ機能を裏付けるものとして、図１５は本発明の原理による新しい制御メッセージ・トランザクションを示す。図１５に示すように、ＣＣＲＱメッセージが識別されたＬＮＳに送信される（また、ハンドオフ処理がＬＮＳに関する情報を新しいＬＡＣに提供しない場合、ハンドオフ処理は、当業技術分野で周知のように新しいＬＡＣが外部ラディアスサーバの助けによってＬＮＳ情報を検索する十分なユーザ情報を新しいＬＡＣに提供しなければならない。すなわち、新しいＬＡＣはラディアスアクセス／応答メッセージにより、ホームラディアスサーバからＬＮＳについて照会する）。ＣＣＲＱメッセージに続いて、ＬＮＳは呼切断通知(Call-Disconnect-Notify)メッセージを古いＬＡＣに送信する。次に、ＬＮＳは、保守の対象となる現行Ｓｒ、Ｓｓを含む継続呼応答(Continued-Call-Reply：CCRP)メッセージによって応答する。最後に、新しいＬＡＣが継続呼接続(Continued-Call Connect：CCCN)によって応答する。

【００６６】上記で説明したように、ＰＰＰ接続は１つのＮＡＳから別のＮＡＳに移転される。新しく定義されたメッセージを裏付けるものとして、以下図５および図６に示されるように対応するＮＡＳについて追加呼状態が定義される。

【表５】

呼状態	イベント	動作	新しい状態
アイドル	ハンドオフ通知	CCRQを送信する	CCRP応答待ち
CCRP応答待ち	CCRPを受信する、承認されない	クリーンアップ	アイドル
CCRP応答待ち	CCRP受信する、承認	CCCNを送信する	確立

表５－新しいＬＡＣ（またはＮＡＳ）

【００６７】観察されるように、継続される呼について新しいＬＡＣ（またはＮＡＳ）に関連するｍＬ２ＴＰの追加された、または新しい呼状態はＣＣＲＰ応答待ち状態である。

【００６８】古いＬＡＣ（またはＮＡＳ）について、確立された状態で呼切断通知(Call-Disconnect-Notify:CDN)メッセージが受信されることに留意されたい。それに応答して、古いＬＡＣは呼をクリーンアップして切断し、アイドル状態に戻る。

【表６】

呼状態	イベント	動作	新しい状態
確立	CCRQを受信した承認されない	エラーコードと共にCCRPを送信するCDNをLNSに送信する	アイドル
確立	CCRPを受信する承認	CDNを古いLACに送信するCCRPを新しいLACに送信する	CCCN待ち
CCCN待ち	CCCNを受信する	データの準備完了	確立
CCCN待ち	CCCNを受信する	クリーンアップ	アイドル

表６－アンカーＬＡＣまたはＬＮＳ

【００６９】観察されるように、継続される呼について、アンカＬＡＣまたはＬＮＳに関連するｍＬ２ＴＰの追加された、または新しい呼状態はＣＣＣＮ待ち状態である。

【００７０】＜ペイロード・メッセージの概観とｍＬ２ＴＰの輻輳制御＞ｍＬ２ＴＰのペイロード・メッセージに関して、サーブＬＡＣとＬＮＳはＬ２ＴＰ手順を遵守する。アンカＬＡＣはペイロード・パケットについてＴｉｄとＣｉｄをスワップする。また、アンカＬＡＣはサーブＬＡＣが送信する（Ｎｒ、Ｎｓ）値を監視する（サーブＬＡＣとアンカＬＡＣの間にはパケット損失が存在するので、アンカＬＡＣのＳｒおよびＳｓの値はどちらもサーブＬＡＣが保守するこれらの数値より遅れると考えられることに留意されたい。）アンカＬＡＣはどちらの方向でもペイロード・パケットの（Ｎｒ、Ｎｓ）を変更しない。アンカＬＡＣは、継続呼要求(Continued-Call-Request)メッセージを新しいサーブＬＡＣから受信する時それ自体のＳｒ、Ｓｓ値だけを利用する。

【００７１】輻輳制御に関して、Ｌ２ＴＰは受信ウィンドウ・サイズを維持する時期、Ｎｒ／Ｎｓを送信する時期およびＡＣＫを送信する時期に関するＬ２ＴＰの要求をｍＬ２ＴＰに適用する。さらに、ｍＬ２ＴＰはサーブＬＡＣとアンカＬＡＣについて次の追加要求を有する。

【００７２】アンカＬＡＣはサーブＬＡＣが送信した（Ｎｒ、Ｎｓ）値の監視が必要である。アンカＬＡＣは、サーブＬＡＣから受信する継続呼接続(Continued-Call-Connect)メッセージに応答する時継続呼応答(Continued-Call-Reply)メッセージの中で保守する（Ｓｒ、Ｓｓ）値を含むべきである。サーブＬＡＣとアンカＬＡＣの間のネットワークは損失が大きいので、アンカＬＡＣが保守するＳｒ値はサーブＬＡＣより遅れることがある。

【００７３】さらに、サーブＬＡＣは、当業技術分野の用語に従えば、単純なレシーバではなく完全なレシーバである。この要求は、ＰＰＰセッションの継続期間中にサーブＬＡＣの変更がある場合、新しいサーブＬＡＣがシーケンス外や重複したパケットを上部層に伝えないということである。

【００７４】簡単に図１６を参照すると、代表的なＮＡＳの高レベル・ブロック図が示される。ＮＡＳは蓄積プログラム制御ベース・プロセッサ・アーキテクチャであり、プロセッサ６５０、メモリ６６０（プログラムの命令と、上記で言及した接続テーブル等のデータを保存する）および経路６６６で表されるように１つかそれ以上の通信機能を結合する通信インタフェース６６５を含む。

【００７５】以上は本発明の原理を例示したものに過ぎず、当業技術分野に熟練した者には、ここで明示的に説明されていなくとも、本発明の原理を実施しその精神と範囲の中にある非常に多くの代替装置が考案できること

を認識することができるだろう。例えば、本発明の概念はサーブＮＡＳが着信呼に関する多重ホップ・トンネルの確立を開始する場合で説明されたが、本発明の概念は、例えば、ＬＮＳが発信呼に関する多重ホップ・シーケンスを開始する場合にも等しく適用できる。こうした修正は簡単明瞭であり、図１７及び図１８で示されているのでここでは説明しない。

【図面の簡単な説明】

【図１】本発明の原理による通信システムを示す図である。

【図２】図１の通信システムを使用する例示としての方法の流れ図を示す図である。

【図３】図１の通信システムを使用する例示としての方法の流れ図を示す図である。

【図４】例示としての多重ホップ・メッセージの流れを示す図である。

【図５】例示としての制御メッセージのトランザクションを示す図である。

【図６】例示としての制御メッセージのトランザクションを示す図である。

【図７】例示としての制御メッセージのトランザクションを示す図である。

【図８】本発明の原理による通信システムの他の実施例を示す図である。

【図９】例示としてのハンドオフ・メッセージの流れを示す図である。

【図１０】図８の通信システムで使用される例示としての方法の流れ図を示す図である。

【図１１】例示としての制御メッセージのトランザクションを示す図である。

【図１２】本発明の原理による通信システムの他の実施例を示す図である。

【図１３】例示としてのハンドオフ・メッセージの流れを示す図である。

【図１４】図１２の通信システムで使用される例示としての方法の流れ図を示す図である。

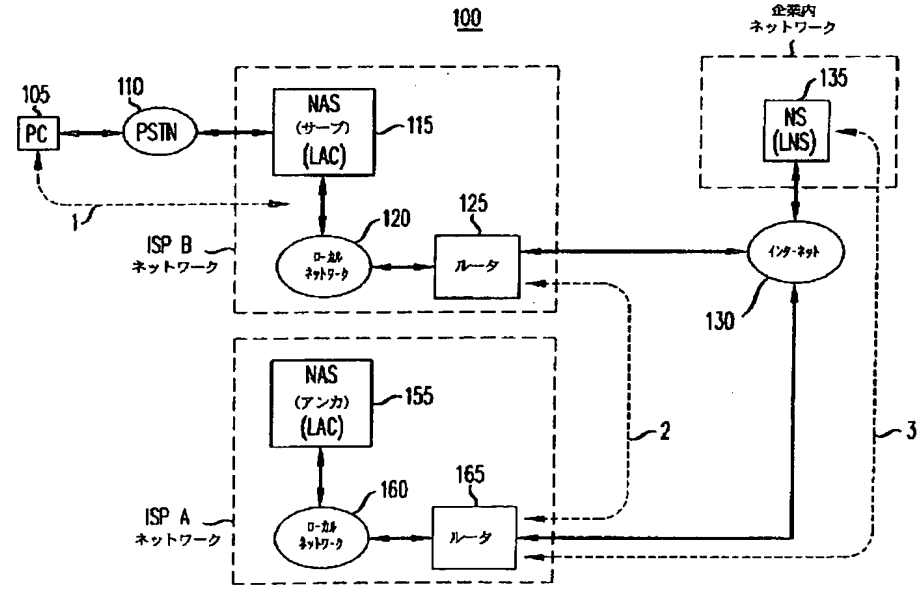
【図１５】例示としての制御メッセージのトランザクションを示す図である。

【図１６】ネットワーク・アクセス・サーバの例示としての高レベル・ブロック図を示す図である。

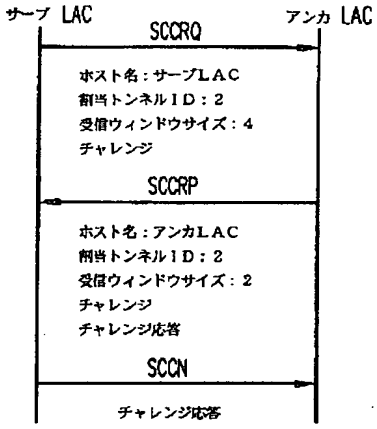
【図１７】発信呼用の例示としての制御メッセージ・トランザクションを示す図である。

【図１８】発信呼用の例示としての制御メッセージ・トランザクションを示す図である。

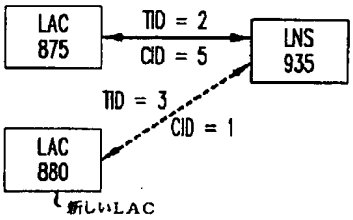
【図１】



【図５】

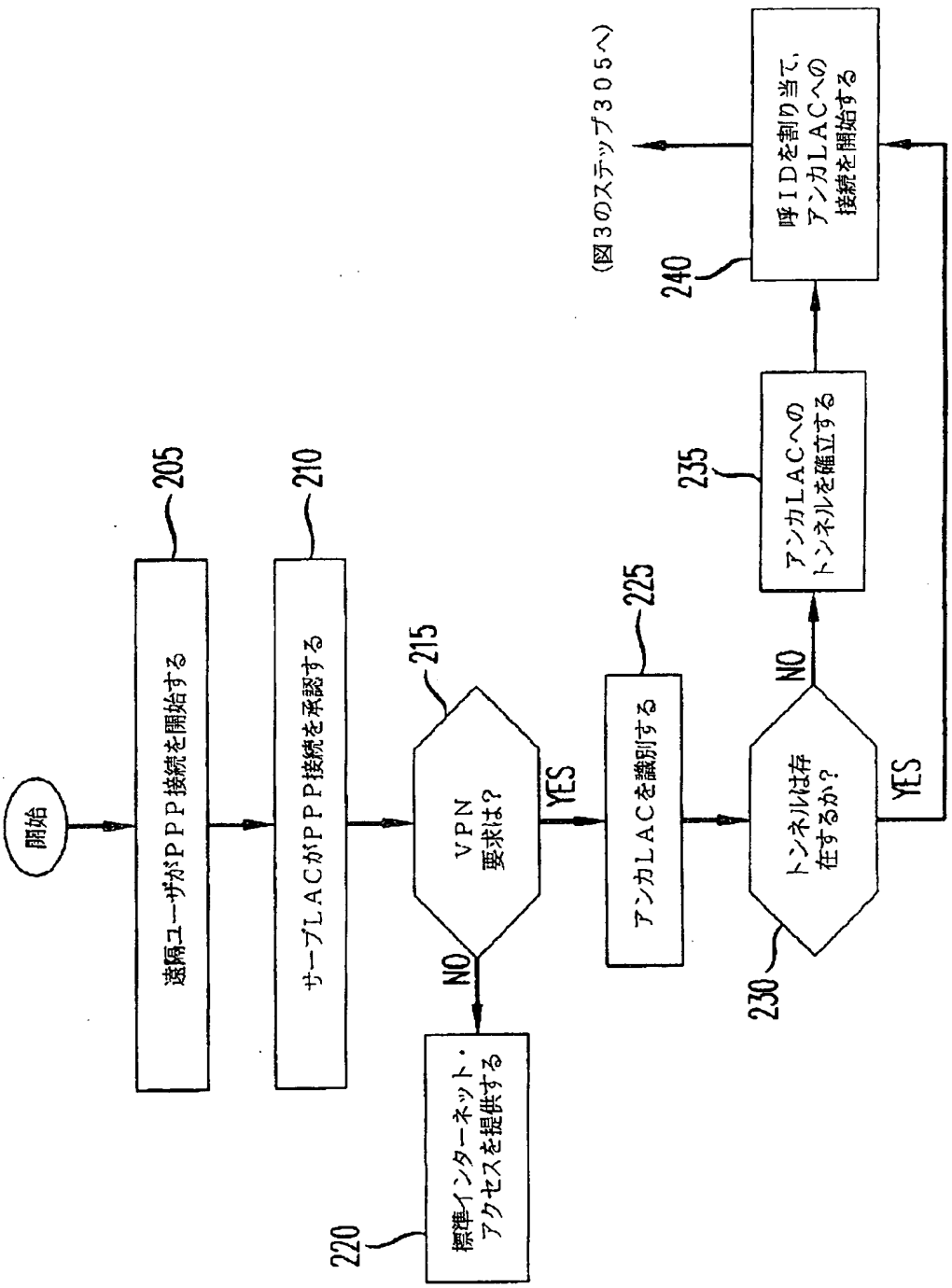


【図１３】

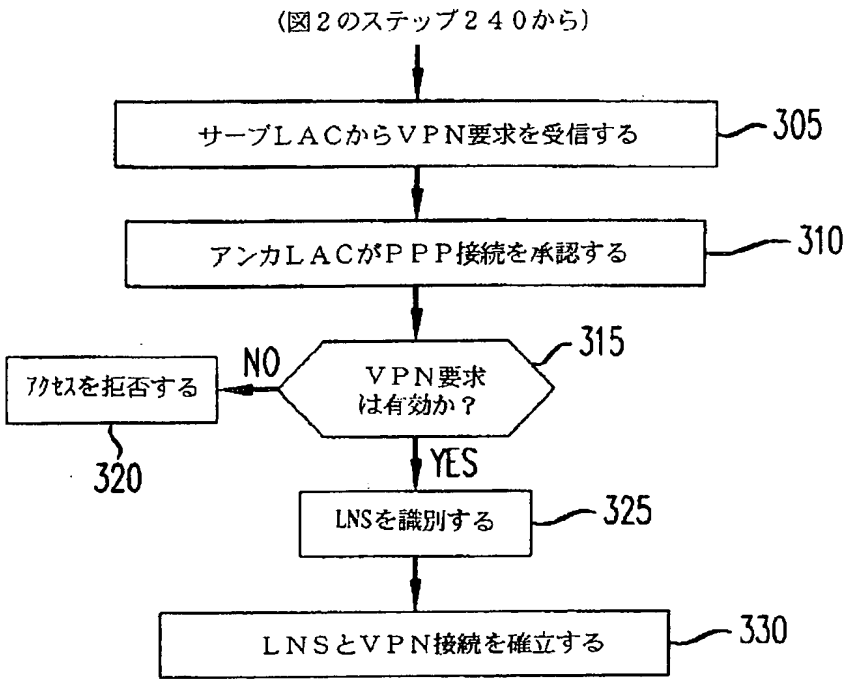


【図４】

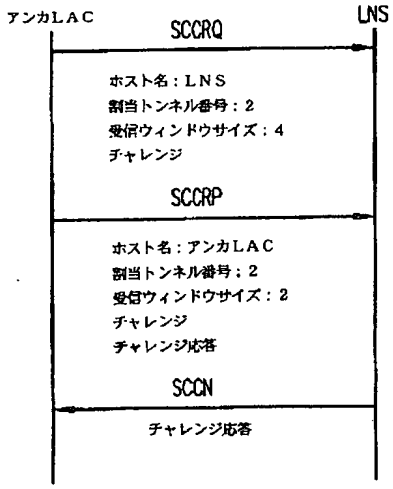
【図２】


開始
遠隔ユーザがＰＰＰ接続を開始する
205
サーブＬＡＣがＰＰＰ接続を承認する
210
ＶＰＮ要求は？
215
YES
NO
標準インターネット・アクセスを提供する
220
アンカＬＡＣを識別する
225
トンネルは存在するか？
230
YES
NO
アンカＬＡＣへのトンネルを確立する
235
呼ＩＤを割り当て、アンカＬＡＣへの接続を開始する
240
（図３のステップ３０５へ）

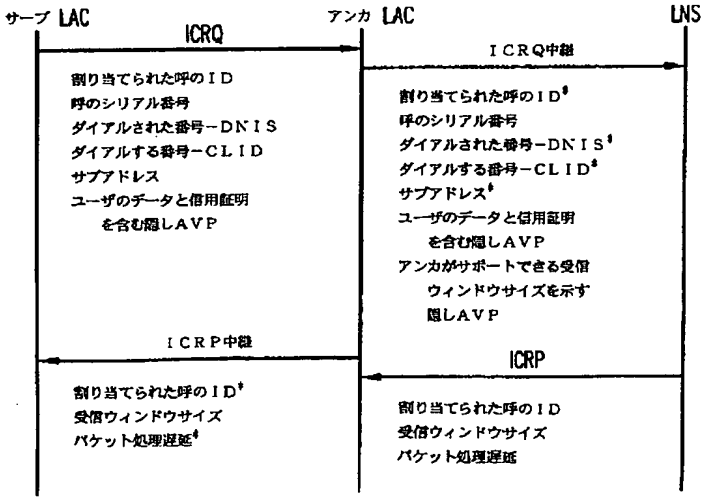
【図３】



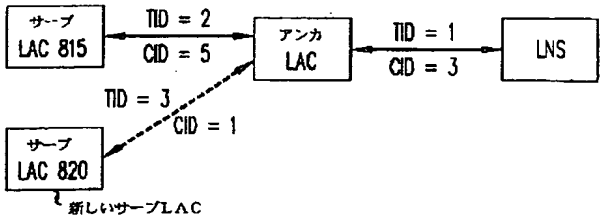
【図１７】



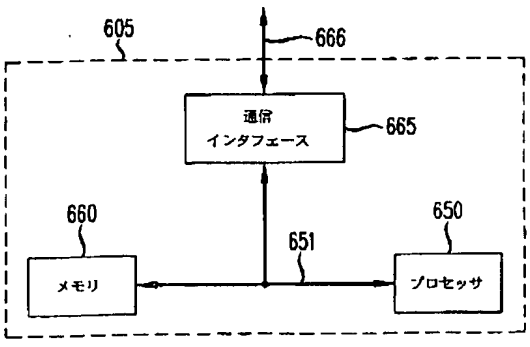
【図６】



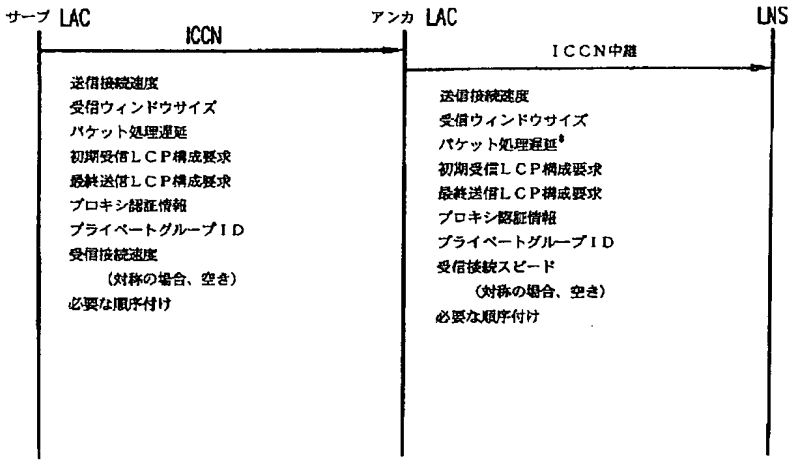
【図９】



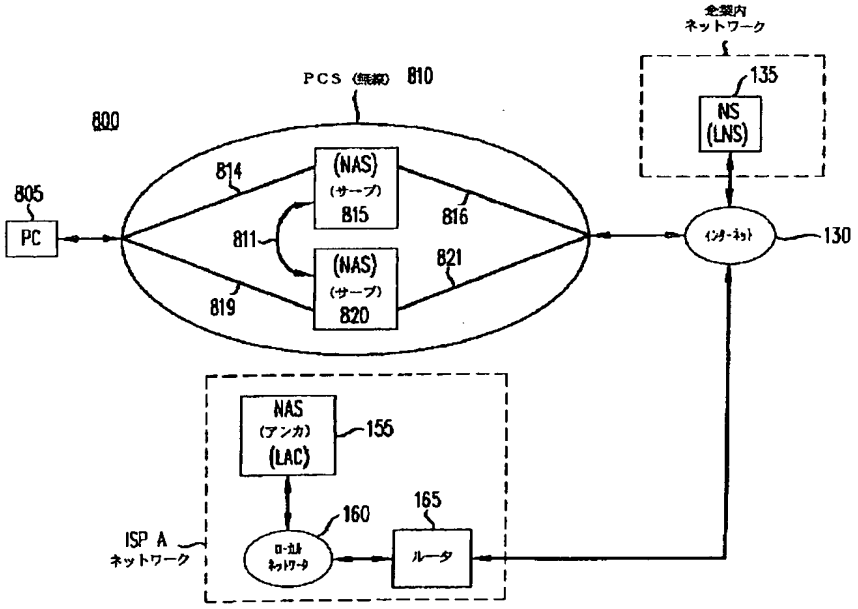
【図１６】



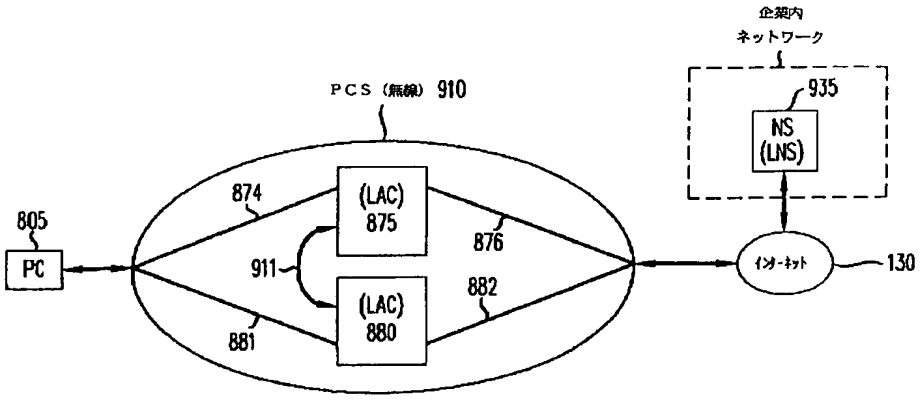
【図７】


サーブ LAC
ICCN
アンカ LAC
ICCN中継
LNS
送信接続速度
受信ウィンドウサイズ
パケット処理遅延
初期受信ＬＣＰ構成要求
最終送信ＬＣＰ構成要求
プロキシ認証情報
プライベートグループＩＤ
受信接続速度
（対称の場合、空き）
必要な順序付け
送信接続速度
受信ウィンドウサイズ
パケット処理遅延
初期受信ＬＣＰ構成要求
最終送信ＬＣＰ構成要求
プロキシ認証情報
プライベートグループＩＤ
受信接続スピード
（対称の場合、空き）
必要な順序付け

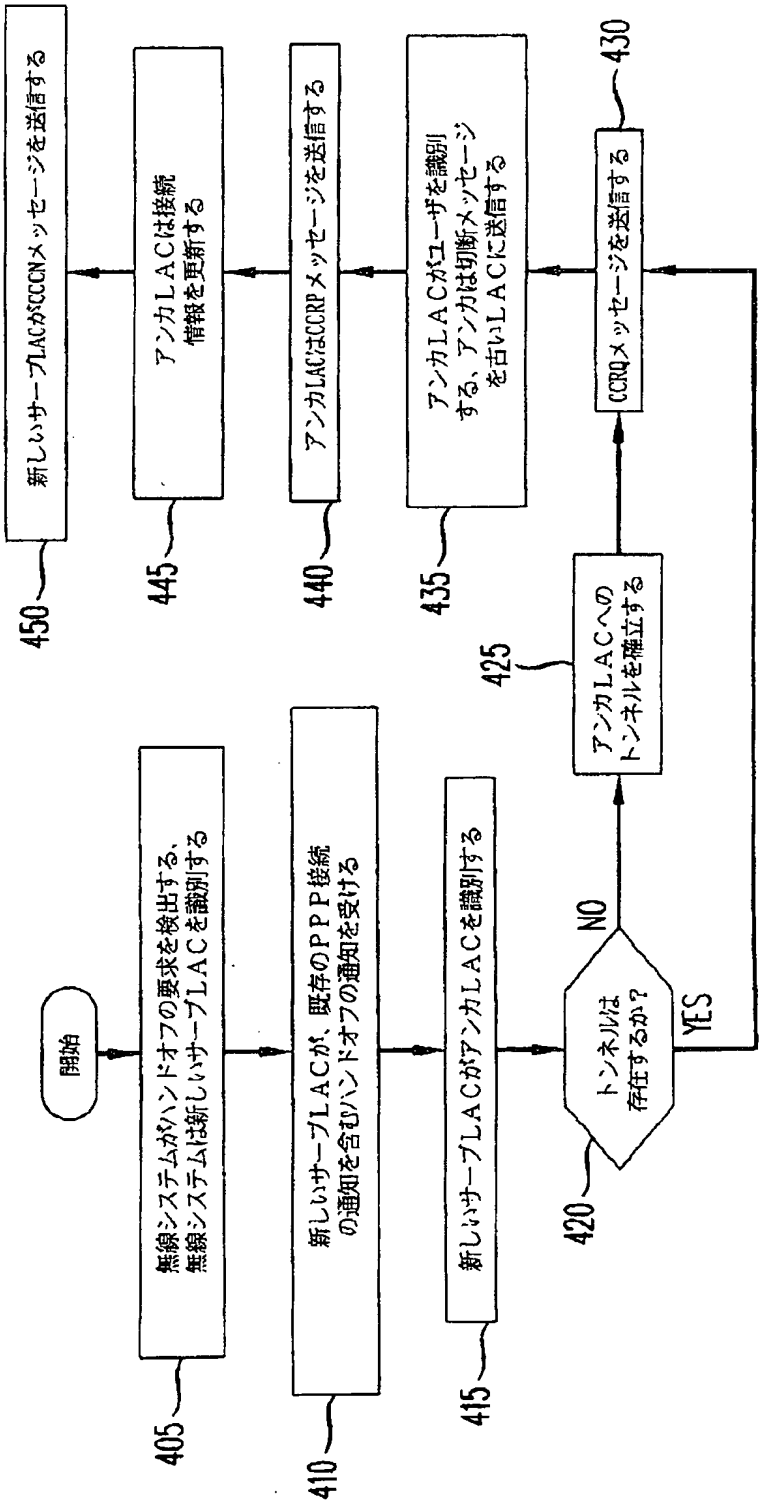
【図８】


企業内
ネットワーク
PCS（無線） 810
800
135
NS
(LNS)
805
PC
814
(NAS)
(サーブ)
815
816
811
(NAS)
(サーブ)
820
821
819
インターネット
130
NAS
(アンカ)
(LAC)
155
160
165
ISP A
ネットワーク
ローカル
ネットワーク
ルータ

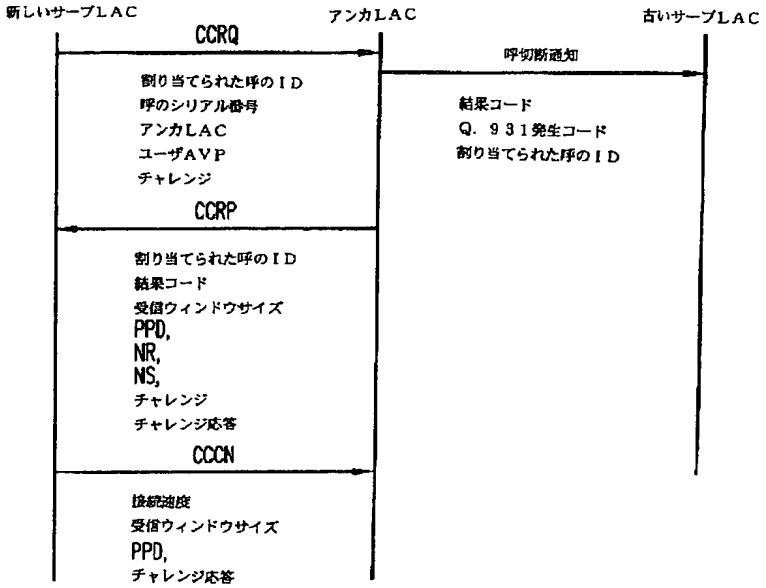
【図１２】


企業内
ネットワーク
PCS（無線） 910
935
NS
(LNS)
874
(LAC)
875
805
PC
876
911
882
(LAC)
880
881
インターネット
130

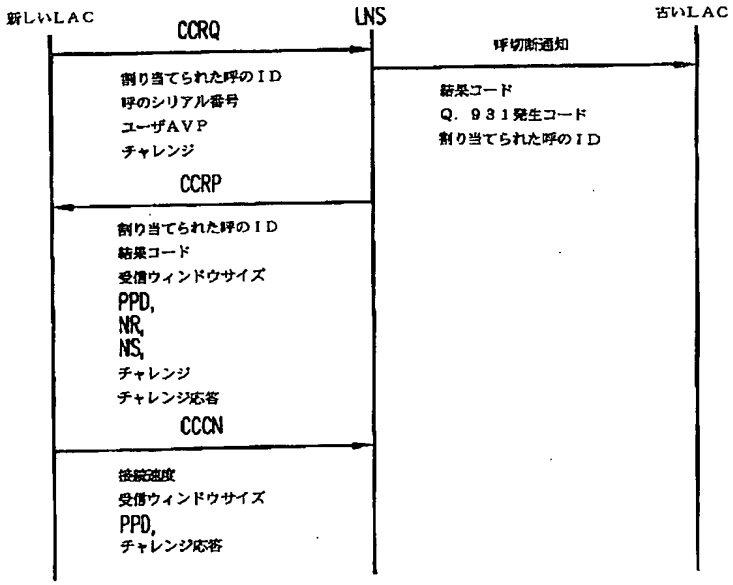
【図１０】


開始
無線システムがハンドオフの要求を検出する、無線システムは新しいサーブLACを識別する
405
新しいサーブLACが、既存のPPP接続の通知を含むハンドオフの通知を受ける
410
新しいサーブLACがアンカLACを識別する
415
トンネルは存在するか?
420
NO
YES
アンカLACへのトンネルを確立する
425
CCRQメッセージを送信する
430
アンカLACがユーザを識別する、アンカは切断メッセージを古いLACに送信する
435
アンカLACはCCRPメッセージを送信する
440
アンカLACは接続情報を更新する
445
新しいサーブLACがCCNメッセージを送信する
450

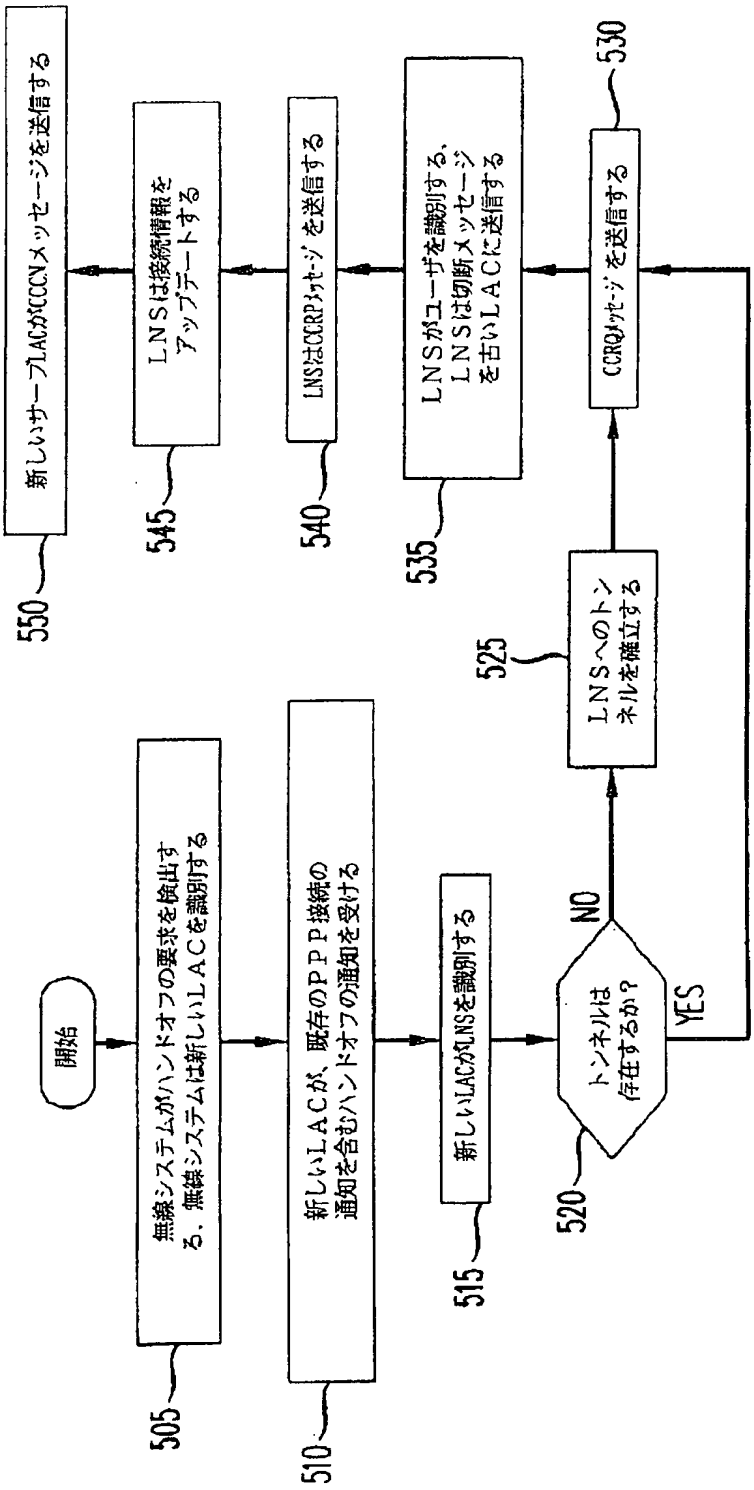
【図１１】


新しいサーブLAC
アンカLAC
古いサーブLAC
CCRQ
割り当てられた呼のＩＤ
呼のシリアル番号
アンカLAC
ユーザAVP
チャレンジ
呼切断通知
結果コード
Q．９３１発生コード
割り当てられた呼のＩＤ
CCRP
割り当てられた呼のＩＤ
結果コード
受信ウィンドウサイズ
PPD,
NR,
NS,
チャレンジ
チャレンジ応答
CCCN
接続速度
受信ウィンドウサイズ
PPD,
チャレンジ応答

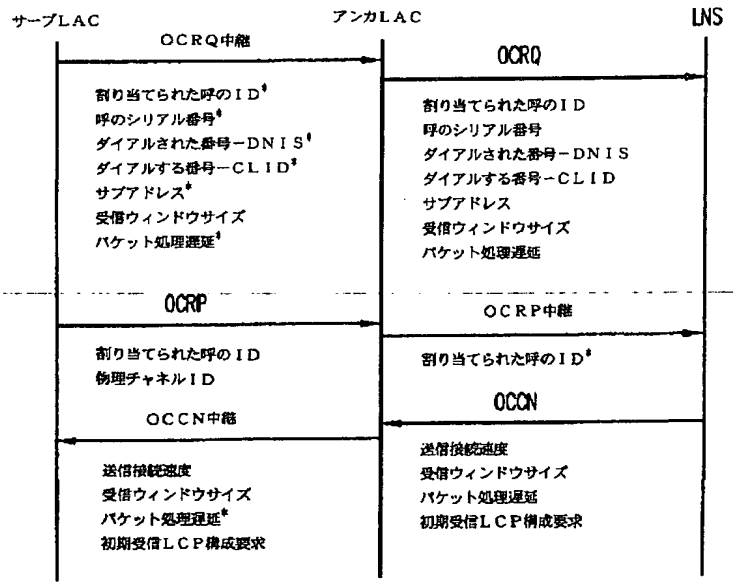
【図１５】


新しいLAC
LNS
古いLAC
CCRQ
割り当てられた呼のＩＤ
呼のシリアル番号
ユーザAVP
チャレンジ
呼切断通知
結果コード
Q．９３１発生コード
割り当てられた呼のＩＤ
CCRP
割り当てられた呼のＩＤ
結果コード
受信ウィンドウサイズ
PPD,
NR,
NS,
チャレンジ
チャレンジ応答
CCCN
接続速度
受信ウィンドウサイズ
PPD,
チャレンジ応答

【図１４】


開始
無線システムがハンドオフの要求を検出する．無線システムは新しいＬＡＣを識別する
505
新しいＬＡＣが、既存のＰＰＰ接続の通知を含むハンドオフの通知を受ける
510
新しいLACがLNSを識別する
515
トンネルは存在するか？
520
NO
YES
LNSへのトンネルを確立する
525
LNSがユーザを識別する．LNSは切断メッセージを古いＬＡＣに送信する
535
LNSはCCRPメッセージを送信する
540
LNSは接続情報をアップデートする
545
新しいサーブLACがCCCNメッセージを送信する
550
CCROメッセージを送信する
530

【図１８】



フロントページの続き

(72)発明者　ギリッシュ　ライ
アメリカ合衆国　60103　イリノイズ，バートレット，レディ　スミス　ロード　523

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１３年7月２７日（２００１．７．２７）

【公開番号】特開平１１－３５５２７２
【公開日】平成１１年１２月２４日（１９９９．１２．２４）
【年通号数】公開特許公報１１－３５５３
【出願番号】特願平１１－１２６５６３
【国際特許分類第７版】
H04L 12/22
12/56
【ＦＩ】
H04L 11/26
11/20 102 A

【手続補正書】
【提出日】平成１２年８月１８日（２０００．８．１８）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　パケット・サーバで使用される方法であって、該方法が、
多重ホップ・パケット・トンネルを他のパケット終端間に確立する段階と、
該多重ホップ・パケット・トンネルを通じて該他のパケット終端間でメッセージを中継する段階とからなることを特徴とする方法。
【請求項２】　請求項１に記載の方法において、該確立する段階が、
１つのパケット終端への第１のパケット・トンネルを確立する段階と、
別のパケット終端への第２のパケット・トンネルを確立する段階とからなることを特徴とする方法。
【請求項３】　請求項２に記載の方法において、該方法はさらに、接続情報を追跡する段階からなり、該接続情報は、該第１のパケット・トンネルに関するトンネル識別値と該第２のパケット・トンネルに関するトンネル識別値とを含むことを特徴とする方法。
【請求項４】　請求項１に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に、該メッセージの少なくとも一部を修正する段階を含むことを特徴とする方法。
【請求項５】　請求項１に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に、該メッセージの少なくとも一部のトンネル識別情報を修正する段階を含むことを特徴とする方法。
【請求項６】　請求項１に記載の方法において、該中継段階は、該他のパケット終端間でメッセージを中継する前に、何れかのメッセージに含まれるパケット処理遅延情報を修正して、該パケット・サーバに関するパケット処理遅延を含ませる段階を含むことを特徴とする方法。
【請求項７】　請求項１に記載の方法において、該パケット・サーバが多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする方法。
【請求項８】　請求項７に記載の方法において、該インターネット・プロトコルがレイヤ２トンネル・プロトコルの形態であることを特徴とする方法。
【請求項９】　パケット・ネットワークで使用される装置であって、該装置はパケット・サーバからなり、該パケットサーバは、
ａ）仮想私設網サービスにアクセスするためにユーザとのポイント・ツー・ポイント・プロトコル接続を承認し、そしてｂ）ホップ間に配置されホップ間でメッセージを中継するように、他のパケット・サーバとの多重ホップ・トンネル接続を承認することを特徴とする装置。
【請求項１０】　請求項９に記載の装置において、該パケット・サーバは、該メッセージの少なくとも一部をホップ間で中継する前に修正することを特徴とする装置。
【請求項１１】　請求項９に記載の装置において、該パケット・サーバは、該メッセージの少なくとも一部のトンネル識別情報をホップ間で中継する前に修正することを特徴とする装置。
【請求項１２】　請求項９に記載の装置において、該パケット・サーバは、ホップ間でメッセージを中継する前に、何れかの該メッセージに含まれるパケット処理遅延情報を修正して、該パケット・サーバに関するパケット処理遅延を含むことを特徴とする装置。
【請求項１３】　請求項９に記載の装置において、該パケット・サーバは、多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする装

置。

【請求項１４】　請求項１３に記載の装置において、該インターネット・プロトコルがレイヤ２トンネル・プロトコルの形態であることを特徴とする装置。